[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 1/00

[12] 发明专利申请公开说明书

[21] 申请号 200410062474.5

[43] 公开日 2005 年 4 月 13 日

[11] 公开号 CN 1605967A

[22] 申请日 2004.7.8
[21] 申请号 200410062474.5
[30] 优先权
[32] 2003.10.10 [33] US [31] 10/683,665
[71] 申请人 国际商业机器公司
地址 美国纽约
[72] 发明人 J·E·阿斯顿 J·M·莱克
D·D·曼纳鲁

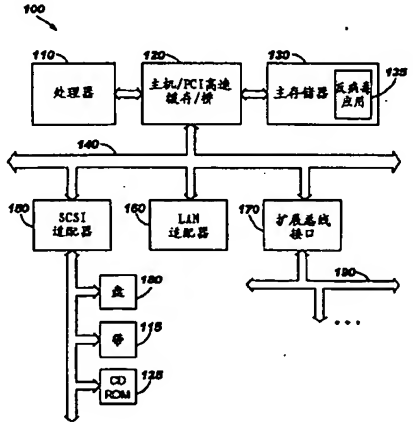
[74] 专利代理机构 北京市中咨律师事务所
代理人 于 静 李 峥

权利要求书 5 页 说明书 9 页 附图 4 页

[54] 发明名称 高效计算机病毒检测系统和方法

[57] 摘要

本发明提供了一种将不同的病毒标记组织为反病毒集合以最小化由于对计算机病毒的扫描而对处理器使用的影响的技术。 所有被分配给一个反病毒集合的病毒标记共享一个共同特征。 随后，所定义的反病毒集合被与一执行媒介相关联，以便每当该执行媒介的目标文件被访问时，对照存储在预先分配的该反病毒集合中的病毒标记扫描该目标文件，以判定该目标文件是否感染了病毒。



ISSN1008-4274

1. 一种计算机可读介质，其中的内容引起计算机系统对与一执行媒介相关的目标文件执行选择性的病毒标记扫描，所述计算机系统具有反病毒程序，该反病毒程序具有指令以执行以下步骤：

将病毒标记组织为多个反病毒集合，其中每一集合包含由该集合中所有病毒标记共享的特征；

将所述多个反病毒集合的一部分与所述执行媒介相关联；以及

扫描所述目标文件的内容以寻找与存储在相关的一个或多个反病毒集合中的病毒标记相匹配的病毒标记。

2. 权利要求 1 的计算机可读介质，进一步包括在所述扫描步骤之前的一步骤，该步骤包括：

将一规则与所述执行媒介相关联以指出所述多个反病毒集合的所述相关部分被应用的方式。

3. 权利要求 1 的计算机可读介质，其中所述相关联步骤包括提供用户可选择的选项。

4. 权利要求 2 的计算机可读介质，其中所述应用的规则包括一个或多个目标文件的定期成批扫描。

5. 权利要求 2 的计算机可读介质，其中所述多个反病毒集合的所述相关部分被应用于执行媒介的目标文件的方式包括调用随后对所述执行媒介的目标文件进行扫描的触发机制。

6. 权利要求 5 的计算机可读介质，其中所述触发机制包括当请求对于所述目标文件的文件操作时应用所述扫描步骤。

7. 权利要求 5 的计算机可读介质，其中所述触发机制包括对与所述执行媒介相关的一个或多个目标文件定期地应用所述扫描步骤。

8. 权利要求 1 的计算机可读介质，进一步包括在所述组织步

骤之前的一步骤，该步骤包括：

确定被安装在所述计算机系统上的多个执行媒介。

9. 权利要求 1 的计算机可读介质，其中所述多个反病毒集合具有第一反病毒集合和第二反病毒集合，所述组织步骤进一步包括：

将所述多个反病毒集合排列为具有第一和第二层的层次结构，所述第一层具有包含可共同地应用于多个执行媒介的病毒标记的所述第一反病毒集合，所述第二层具有包含可排他地应用于所述多个执行媒介的第一部分的病毒标记的所述第二反病毒集合。

10. 权利要求 1 的计算机可读介质，

其中所述多个反病毒集合具有第一反病毒集合、第二反病毒集合、及第三反病毒集合，

其中所述多个执行媒介具有第一部分，

其中所述组织步骤进一步包括：

将所述多个反病毒集合排列为具有第一层、第二层、和第三层的层次结构，所述第一层具有包含可共同地应用于所述多个执行媒介的病毒标记的所述第一反病毒集合，所述第二层具有包含可共同地应用于所述多个执行媒介的所述第一部分的病毒标记的所述第二反病毒集合，所述第三层具有包含可排他地应用于所述多个执行媒介的所述第一部分中的一个的病毒标记的所述第三反病毒集合。

11. 一种用于对与一执行媒介相关的目标文件执行选择性的病毒标记扫描的计算机系统，具有一反病毒程序的该计算机系统包括：

用于将病毒标记组织为多个反病毒集合的装置，其中每一集合包含由该集合中所有病毒标记共享的特征；

用于将所述多个反病毒集合的一部分与所述执行媒介相关联

的装置；以及

用于扫描所述目标文件的内容以寻找与存储在相关的一个或多个反病毒集合中的病毒标记相匹配的病毒标记的装置。

12. 权利要求 11 的计算机系统，进一步包括：

用于将一规则与所述执行媒介相关联以指出所述多个反病毒集合的所述相关部分被应用的方式的装置。

13. 权利要求 12 的计算机系统，其中所述规则包括一个或多个目标文件的定期成批扫描。

14. 权利要求 12 的计算机系统，其中所述多个反病毒集合的所述相关部分被应用于执行媒介的目标文件的方式包括用于激活所述用于扫描的装置的触发机制。

15. 权利要求 14 的计算机系统，其中所述触发机制包括当请求对于所述目标文件的文件操作时激活所述用于扫描步骤的装置。

16. 权利要求 14 的计算机系统，其中所述触发机制包括对与所述执行媒介相关的一个或多个目标文件定期地应用所述扫描步骤。

17. 权利要求 11 的计算机系统，进一步包括：

用于确定被安装在所述计算机系统上的多个执行媒介的装置。

18. 权利要求 11 的计算机系统，其中所述多个反病毒集合具有第一反病毒集合和第二反病毒集合，所述用于组织的装置进一步包括：

用于将所述多个反病毒集合排列为具有第一和第二层的层次结构的装置，所述第一层具有包含可共同地应用于多个执行媒介的病毒标记的所述第一反病毒集合，所述第二层具有包含可排他地应用于所述多个执行媒介的第一部分的病毒标记的所述第二反病毒集合。

19. 权利要求 11 的计算机系统，

其中所述多个反病毒集合具有第一反病毒集合、第二反病毒集合、及第三反病毒集合，

其中所述多个执行媒介具有第一部分，

其中所述用于组织的装置进一步包括：

用于将所述多个反病毒集合排列为具有第一层、第二层、和第三层的层次结构的装置，所述第一层具有包含可共同地应用于所述多个执行媒介的病毒标记的所述第一反病毒集合，所述第二层具有包含可共同地应用于所述多个执行媒介的所述第一部分的病毒标记的所述第二反病毒集合，所述第三层具有包含可排他地应用于所述多个执行媒介的所述第一部分中的一个的病毒标记的所述第三反病毒集合。

20. 一种用于对与一执行媒介相关的目标文件执行选择性的病毒标记扫描的方法，包括：

将病毒标记组织为多个反病毒集合，其中每一集合包含由该集合中所有病毒标记共享的特征；

将所述多个反病毒集合的一部分与所述执行媒介相关联；以及

扫描所述目标文件的内容以寻找与存储在相关的一个或多个反病毒集合中的病毒标记相匹配的病毒标记。

21. 权利要求 20 的方法，进一步包括在所述扫描步骤之前的一步骤，该步骤包括：

将一规则与所述执行媒介相关联以指出所述多个反病毒集合的所述相关部分被应用的方式。

22. 权利要求 21 的方法，其中所述规则包括一个或多个目标文件的定期成批扫描。

23. 权利要求 20 的方法，其中所述相关联步骤包括提供用户可选择的选项。

24. 权利要求 21 的方法，其中所述多个反病毒集合的所述相

关部分被应用于执行媒介的目标文件的方式包括用于随后对所述执行媒介的目标文件进行扫描的触发机制。

25. 权利要求 24 的方法，其中所述触发机制包括当请求对于所述目标文件的文件操作时应用所述扫描步骤。

26. 权利要求 24 的方法，其中所述触发机制包括对与所述执行媒介相关的一个或多个目标文件定期地应用所述扫描步骤。

27. 权利要求 20 的方法，进一步包括在所述组织步骤之前的一步骤，该步骤包括：

确定被安装在所述计算机系统上的多个执行媒介。

28. 权利要求 20 的方法，其中所述多个反病毒集合具有第一反病毒集合和第二反病毒集合，所述组织步骤进一步包括：

将所述多个反病毒集合排列为具有第一和第二层的层次结构，所述第一层具有包含可共同地应用于多个执行媒介的病毒标记的所述第一反病毒集合，所述第二层具有包含可排他地应用于所述多个执行媒介的第一部分的病毒标记的所述第二反病毒集合。

29. 权利要求 20 的方法，

其中所述多个反病毒集合具有第一反病毒集合、第二反病毒集合、及第三反病毒集合，

其中所述多个执行媒介具有第一部分，

其中所述组织步骤进一步包括：

将所述多个反病毒集合排列为具有第一层、第二层、和第三层的层次结构，所述第一层具有包含可共同地应用于所述多个执行媒介的病毒标记的所述第一反病毒集合，所述第二层具有包含可共同地应用于所述多个执行媒介的所述第一部分的病毒标记的所述第二反病毒集合，所述第三层具有包含可排他地应用于所述多个执行媒介的所述第一部分中的一个的病毒标记的所述第三反病毒集合。

高效计算机病毒检测系统和方法

技术领域

本发明一般涉及用于检测计算机病毒的改进的系统和方法，更特别地，涉及用于提供自动的和用户可选的机制的有利技术，该机制用于按照软件应用来组织包含病毒标记（virus signature）的反病毒集合，以最小化由于扫描计算机病毒而产生的对处理器使用的影响。

背景技术

通常，目前的计算机反病毒软件程序花费大量的时间对照已过时的病毒标记检查计算机文件。计算机病毒通常利用诸如AIX®、LINUX®、Windows®或类似的操作系统以及诸如Java™虚拟机、Visual Basic或类似的解释程序中的漏洞。病毒还利用在诸如Microsoft® Outlook®、Microsoft® Excel或类似的现成的软件应用中发现的漏洞。然而，随着时间的流逝，新版本的操作系统、解释程序、以及软件应用解决了那些以前的漏洞，使得很多病毒标记变得不相关了。

此外，现有的50,000种病毒中的多数病毒是针对于在Windows®操作系统或被定制在Windows®上运行的流行软件应用版本中的漏洞。虽然Windows®操作系统可能是相当普遍的，但是许多企业也在运行其他操作系统的计算机上运行流行软件应用版本。这些企业通常为了安全目的需要在他们的计算机上运行反病毒软件程序。很多这些运行在非Windows®操作系统上的典型反病毒程序仍然对照针对在Windows®上运行的软件应用版本定制的病毒标记扫描文件。当对文件应用不相关的标记时，诸如处理器使用、存储器、存储设备及类似的计算机资源就被不必要地被消耗了。应当注意这里使用的术语Windows®指由Microsoft®公司开发的包括XP、

XP专业版、NT等的Windows®操作系统系列。

显然地，当大部分标记是无关的并依赖于应用反病毒程序的环境时，针对每个新文件检查50,000种病毒标记会导致计算机资源的低效使用。因此需要对计算机病毒提供更有效检测的系统和方法。

发明内容

在本发明的几个方面之中，本发明提供了一种用于将病毒标记组织为反病毒集合的机制，其中每一集合包含由该集合中所有病毒标记共享的特征。当一个执行媒介进行程序启动时，与包含用于该可执行程序的病毒标记的相关反病毒集合有关的反病毒程序验证该可执行程序的完整性。通过利用特定执行媒介与反病毒集合的相关性，实时反病毒程序通过将病毒检测器聚焦于对该操作环境所定制的病毒，来有利地利用计算机资源。

本发明的另一方面包括提供可由用户修改以进一步指定利用病毒标记扫描病毒载体的范围和层次的表。

本发明的另一方面包括提供将一些规则指派给一可执行程序以控制反病毒集合应用到该可执行程序的目标文件的方式。

根据下面详细的说明和附图，对本发明更加完全的理解，以及本发明的进一步特征和优点将是显然的。

附图说明

图1显示在其中本发明可被适当地实现的示例性计算机系统的方框图；

图2是说明根据本发明的优选实施例的计算机系统的特定示例的功能性软件部件的方框图；

图3显示用于根据本发明的划分病毒标记的示例性数据库关系图；以及

图4是说明根据本发明的检测计算机病毒的方法的流程图。

具体实施方式

图 1 显示说明在其中本发明可被适当地实现的计算机的方框图。计算

机 100 可以适宜地是手持计算机、笔记本、服务器或任何其他需要保护免受计算机病毒之害的基于处理器的机器。如图所示的计算机使用外围部件互连（PCI）局部总线体系结构。虽然显示了 PCI 总线，但诸如加速图形端口（AGP）和工业标准体系结构（ISA）的其他总线体系结构也可被使用.处理器 110 和主存储器 130 通过 PCI 桥 120 连接到 PCI 局部总线 140。PCI 桥 120 也可以包括集成的存储器控制器和用于处理器 110 的高速缓冲存储器。在所示的例子中，小型计算机系统接口（SCSI）主机总线适配器 150、局域网（LAN）适配器 160、以及扩展总线接口 170 通过直接部件连接被连接到 PCI 局部总线 140。扩展总线接口 170 提供到用于其他未显示的外围设备的扩展总线 190 的连接。SCSI 主机总线适配器 150 提供对于硬盘驱动器 180、磁带驱动器 115 和 CD-ROM 驱动器 125 的连接。一操作系统运行于处理器 110 上并被用于对计算机 100 中的各种部件进行协调和提供控制。该操作系统可以是可购买到的操作系统，诸如 AIX®、LINUX®、Windows®、Windows®CE3.0 等。诸如 Java™、Object Oriented Perl、或 Visual Basic 的面向对象的编程系统可与操作系统一起运行并提供自计算机 100 中的处理器 110 执行的 Java™ 程序或应用对操作系统的调用。用于操作系统、面向对象的操作系统、以及诸如本发明的应用或程序的指令位于诸如盘 180 或网络服务器的存储设备上，并可以被加载到主存储器 130 中以供处理器 110 执行。反病毒应用 135 包含根据如图 1 的实施例中所说明的本发明要执行的指令。这些指令实现的步骤有诸如将病毒标记组织为多个反病毒集合，其中每一集合包含由该集合中所有病毒标记所共享的特征，将该多个反病毒集合的一部分与执行媒介相关联，以及响应由该执行媒介所引发的触发机制，扫描目标文件的内容以寻找与存储在所述相关的一个或多个反病毒集合中的病毒标记相匹配的病毒标记。处理器 110 一般可以运行于 200Mhz 或更高频率。

本领域的普通技术人员将理解图1中的硬件可根据具体实施而变化。其他的内部硬件或外围设备，诸如闪速ROM或等效的非易失性存储器等，可被用于附加于或替代图1中所示的硬件。并且，本发明的过程也可被应用于

多处理器数据处理系统。

图1中所示的例子和以下所述的示例并不意味着对本发明体系结构的限制。

图2示出了一个说明示例性软件功能部件的方框图，该些软件功能部件可被适宜地应用于根据本发明的图1中所示的计算机系统。本领域的普通技术人员将理解在软件应用220、操作系统210，及反病毒检测应用240中采用的指令操作由例如图1的处理器110的处理器来执行。本领域的普通技术人员将认识到，本发明的许多实施例也是可行的，且显示在图2中的例子是为了说明的目的被显示的，并不限制本发明的范围。

计算机系统200包括一个或多个软件应用220，具有文件操作工具230的操作系统210，和具有关联表250的反病毒检测应用240。软件应用220代表定制软件应用和诸如Lotus1-2-3®、Freelance® Graphics、Microsoft® Word等的现成软件。文件225由运行着的软件应用220创建或可由其读取。文件225可能已由计算机系统200，或由随后通过局域网或因特网等将它们传送给计算机系统200的另一个计算机系统所创建。计算机病毒可能被也称作执行媒介的软件应用220、或者被也称作目标文件的文件225所携带。如有关图1的说明中所描述的，操作系统210可以是可购买到的。可选地，操作系统210可包括Java™虚拟机、或其他类似的解释软件部件。文件操作工具230通过接收文件操作请求然后在诸如盘、磁带、CD ROM、LAN适配器等硬件设备上满足这些请求，来控制计算机系统200中的文件的文件管理。例如，每当软件应用220需要打开、创建、删除、读或写文件时，软件应用220就向文件操作工具230发出其请求。当接收到请求时，文件操作工具230就在相关的硬件设备上打开该文件。

反病毒检测应用240含有规则引擎245和用于存储并向执行媒介指派规则和反病毒集合的关联表250。在图2所示的例子中，关联表250含有至少3列260A-C和表示表250中的记录的行265A-D。列260A包括已知的可被安装在计算机系统200中的执行媒介。例如，用于Windows® XP的1-2-3版本4已被输入在行265A、列260A的字段内，用于Linux®的1-2-3版本4已被输入

在行265B、列260B的字段内，电子数据表格应用A已被输入在行265C、列260C的字段内，及通配符“*”已被输入在行265D、列260A的字段内。

如图2所示，表250对于在不同操作系统上的相同应用的不同版本例如用于XP的1-2-3®和用于Linux®的1-2-3®可具有不同项，这允许反病毒应用基于执行媒介所运行的操作环境来扫描应用。尽管没有示出，表250允许用于相同应用的不同版本的不同项被分配给不同的病毒标记集合。此指派机制允许当目标文件由已修复了在以前版本中发现的漏洞的较近版本的执行媒介打开时，根据本发明的反病毒应用免除由利用以前的漏洞的病毒标记扫描目标文件。

列 260A 内的字段项可由反病毒检测应用 240 利用已知的技术例如搜索盘驱动器以确定哪些应用已被安装在计算机系统 200 上，来自动填充。例如，在 Windows®操作环境下，可扫描 Windows® 注册表来发现已安装应用的存在。特别地，著名的应用已公布了表示该应用名称、版本等的标记以允许通过扫描盘驱动器、注册表等以发现这些所公布的标记，来填充表 250，而无需用户交互。另外，当应用被安装或当应用执行时，应用项可自动在列 260A 中填充字段项。类似地，反病毒应用 240 允许用户拥有适当的权利以修改各项及向表 250 添加其他记录。

列260B包括含有一个或多个要以由在列260C中指定的一个或多个规则所定义的方式被应用的病毒标记的反病毒集合的名称。列260C可选地包括一个或多个驱动规则引擎245以指示相关的反病毒集合应当怎样和什么时候被应用的规则。例如，一规则可以包括一个指示，即每当被列于列260A中的执行媒介打开一个目标文件时，通过应用在用于该执行媒介的反病毒集合中发现的病毒标记来扫描该目标文件。其他规则可描述扫描发生的方式。例如，可指定将引起扫描计算机系统200的文件系统中与一指定执行媒介相关联的所有目标文件的定期方式，而不是当文件打开时触发扫描。

其他规则可指定相关病毒标记的覆盖范围。考虑到文件一般包括在创建时由操作系统分配的唯一文件标识符，规则可以指定当应用所指派的反病毒集合时排除在外或包含在内的目标文件的文件标识符。作为另一个例

子，规则可被指定以跟踪先前已被扫描过的目标文件以免除冗余的扫描。

回过来参照在行265D、列260A的通配符项，支持通配符项允许本发明对于未列出或不知道的应用来定制病毒扫描。正如对于已知的通配符匹配，字符的组合被匹配于通配符以确定一个匹配。例如，项“*”将匹配未列于列260A中的任何执行媒介，而项“Word*”将匹配所有的与版本或操作环境无关的Word应用。这样一种方案提供了定制对由执行媒介所携带的病毒进行病毒扫描的手段。

存在许多已知的描述一个典型的反病毒应用怎样连接到操作系统的技术。例如，一个已知技术包括每当文件操作工具230对一个目标文件发出文件打开指令时触发反病毒检测应用240的操作。例如，每当操作系统被调用以发出一个用以打开文件的函数，例如fopen()函数调用时，在软件应用220发出任何读或写请求之前，操作系统调用反病毒检测应用240。一旦被触发，在将环境返回给该fopen()函数之前，反病毒检测应用240可应用列于列260B中的不同的反病毒集合。

每当执行媒介的指令开始执行时，操作系统实例化运行该执行媒介的运行进程。该运行进程包括如列260A中所描述的与该执行媒介相关的应用标记。操作中，本发明将在该运行进程中发现的应用标记与列260A中的项相比较，以确定是否存在与表250中特定行的匹配。如果存在匹配，与该匹配的执行媒介相关的随后的目标文件将依照在被输入到列260B中的反病毒集合中发现的所有病毒标记被扫描。如以下有关图3的讨论所述的扫描的层次和范围可按列260C中的规则来指定。

如果列260C为空，反病毒检测应用240利用存储在显示于列260B中的反病毒集合中的所有病毒标记扫描目标文件。如果260C中存在一个或多个规则，列于列260C中的该一个或多个规则被规则引擎245评估并应用。

存在关联表250的不同的实施例。关联表250可以实现为文件、数据库等。此外，列260B中的项示出了反病毒集合例如AV1、AV2和AV3的分配。这些反病毒集合可实现为计算机文件，或在优选实施例中被组织到数据库中。本发明将通常提供关联表250的项的默认值。然而，用户可通过使用图

形用户界面或在表250的实现为计算机文件的情况下使用文件编辑工具来修改该关联表250。

图3显示根据本发明划分病毒标记的示例性数据库关系图300。在图3中，数据库关系图300示出了排列的三个层次。第一层包含病毒标记集合310。第二层包含病毒标记集合320、330、340。第三层包含病毒标记集合350、360和370。在一集合中发现的每一个病毒标记与在该集合中发现的所有其他病毒标记共享一共同特征。此特征在下文中被进一步描述。注意，排列的其它层以及每一层的其它集合都是可能的。图3旨在作为一个说明性例子，并无意限制本发明的范围。

集合310包含利用在所有执行媒介中发现的共同漏洞的所有共同病毒标记的集合。集合320包含仅利用在应用1中发现的漏洞的所有病毒的病毒标记的集合。例如，如果集合320在关联表250中被指派给应用1，则扫描被应用1访问的目标文件所需的相关病毒标记，除了那些在集合310中发现的标记，即对所有应用共同的病毒标记之外，将包括那些在集合320中发现的病毒标记。集合320和集合310之间的这种关系由链接315所建立。集合330包含仅利用在一特定商业应用套件中发现的漏洞的共同病毒标记的集合。例如，如果集合330在关联表250中被指派给一个应用，则集合330通过链接325引用集合310以允许应用除了对于该商业应用套件共同的病毒标记之外对于所有应用共同的病毒标记。集合340包含仅利用在应用2中发现的漏洞的所有病毒标记的集合，并通过链接335引用集合310。集合350包含仅利用在一般被打包到商业应用套件中的电子数据表格应用中发现的漏洞的所有病毒标记的集合，并通过链接355引用集合330。集合360包含仅利用在一般被打包到商业应用套件中的字处理应用中发现的漏洞的所有病毒标记的集合，并通过链接365引用集合330。集合370包含仅利用在一般被打包到商业应用套件中的画图应用中发现的漏洞的所有病毒标记的集合，并通过链接375引用集合330。

通常，集合的大小随着沿该层次结构下降而减小，以致于集合310中的病毒标记的数量将少于集合330中病毒标记的数量且集合330中病毒标记的数量将少于集合360中病毒标记的数量。

作为例子，在例如表250的关联表中用于电子数据表格应用A的项将包括引用集合350的指示。在本发明的运行期间，每当电子数据表格被打开或被写入文件系统时，将对照存储在集合350中病毒标记、存储在集合330中的病毒标记和存储在集合310中的病毒标记扫描该电子数据表格。例如，如果集合330被指派给画图应用，则仅将使用集合330和310中的病毒标记。将病毒标记的集合排列为层次结构通过免除了多余的反病毒集合的规定而提供了高效的存储器利用。这种排列也允许通过指派来自特定的层的所希望的一组来改变覆盖范围。例如，用户可能只想对一般被打包到一商业应用套件中的应用来应用对于该整个商业应用套件共同的病毒标记。在这种情况下，用户将把集合330指派到包含例如画图应用标记和字处理标记的记录的列260B。可提供未示出的第4层，以包括例如一字处理应用的不同版本。添加第4层将允许用户指定对于字处理应用的所有版本共同的病毒标记，或者对于字处理应用的所有版本共同的病毒标记，以及特定于特殊版本的病毒标记。注意，如此处所使用的术语“用户”包括但不限于执行媒介的最终用户、信息技术专家和网络管理员等。

注意，链接315、325、335、355、365和375可以是双向的以允许用户为执行媒介指定特定的集合例如集合330，并使来源于集合330的集合中的病毒标记被应用到该执行媒介的目标文件。该操作是另一个被在列260C中指定的规则可实现什么操作的示例。本领域的普通技术人员也应当认识到存在许多将病毒标记集合组织为层次结构的实施方式，并且图3中所示的示例性组织不意味着限制本发明的范围。

图4示出说明根据本发明检测计算机病毒的方法的流程图400。在步骤410，在不同的执行媒介与一反病毒集合之间作出关联。该关联可由用户预先指定或进行更改。在步骤420，本发明被设定为基于执行于操作系统或解释程序的环境下的文件操作来触发扫描操作。其他已知的触发技术也是可获得且可应用的。在步骤430，当操作系统试图代表相关执行媒介对目标文件执行文件操作时，本发明截取该文件操作以便执行根据本发明的指令。虽然该实时扫描技术每当新文件已被打开时试图立即检测病毒，但根据本发明可使用其他技术，例如定期成批扫描。通过对于所需的执行媒介将定

期成批扫描规则输入到列260C中，可实现基于每一执行媒介的成批扫描。

在可选步骤450，本发明检验是否已定义免除扫描该目标文件的规则。例如，一规则的作用可以是不重新扫描那些已被扫描过的目标文件。如果存在被定义为免除扫描该目标文件的规则，则进入步骤496，在其中本发明允许文件操作继续且本发明休眠。如果没有被定义为免除扫描的规则，则本发明前进到步骤460。在步骤460，本发明判定该执行媒介是否具有任何相关的反病毒集合。如果不存在相关的反病毒集合，则进入步骤470，在其中提供一可选默认行为。例如，对照所有存储的反病毒集合，扫描目标文件和执行媒介。如果存在相关的集合，则本发明前进到步骤480，在其中对照存储在该反病毒集合中的病毒标记扫描目标文件。注意，对照特定的病毒标记扫描目标文件的方式对本领域的普通技术人员来说是公知的。扫描步骤470和480的结果在步骤490中被分析。步骤490判定前一扫描是否发现了嵌入的病毒。如果没有嵌入的病毒，则本发明前进到可选步骤494。在步骤494，目标文件被标记以指示该文件已被成功扫描，然后前进到步骤496。如果在步骤490在目标文件中发现了嵌入病毒，则本发明前进到步骤492。在步骤492，可对目标文件执行各种恢复操作。可通知用户并向用户提供选项。此类恢复选项包括隔离或删除感染的文件。

应该理解，虽然在本发明优选实施例中反病毒应用被以软件来实现，但在本发明的其他实施例中，被软件部分执行的全部或部分指令步骤可存在于与一个或多个计算机相连的固件或其他程序介质中，其中这些计算机可运行以与对目标文件进行操作的计算机系统进行通信。

本发明的说明已基于说明和解释的目的被呈现，且并不意味着是穷举的和以所公开的形式限制本发明。许多修改和变换对本领域技术人员来说是明显的。被选出和描述的实施例是为了更好地解释本发明的原理、其实际应用，并使本领域的其他普通技术人员理解本发明。在权利要求的限制下，使本发明适应特定环境或用户所需的具有各种修改的各种实施例都是预期中的，包括但不限于依据迅速发展的硬件和软件部件和技术对此处各种教导的改造。

图1

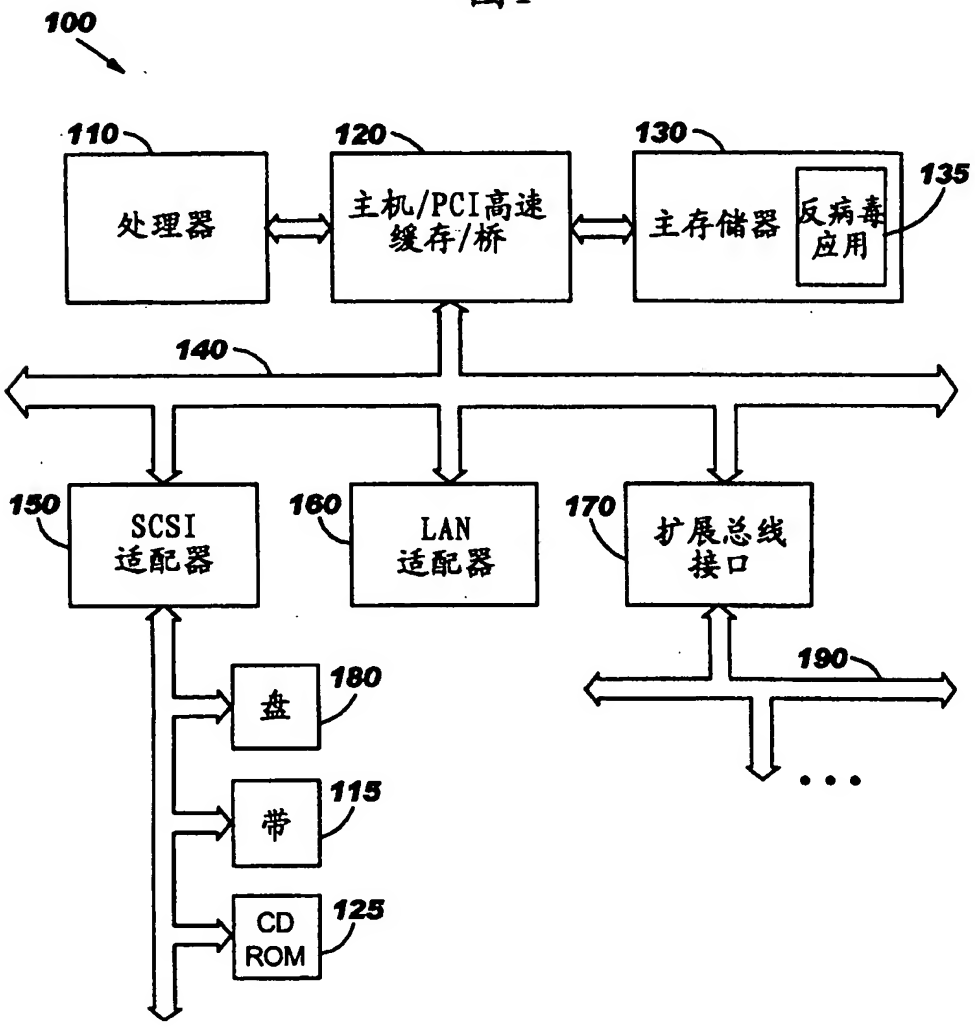

100
110
处理器
120
主机/PCI高速缓存/桥
130
主存储器
反病毒应用
135
140
150
SCSI适配器
160
LAN适配器
170
扩展总线接口
180
盘
115
带
125
CD ROM
190

图2

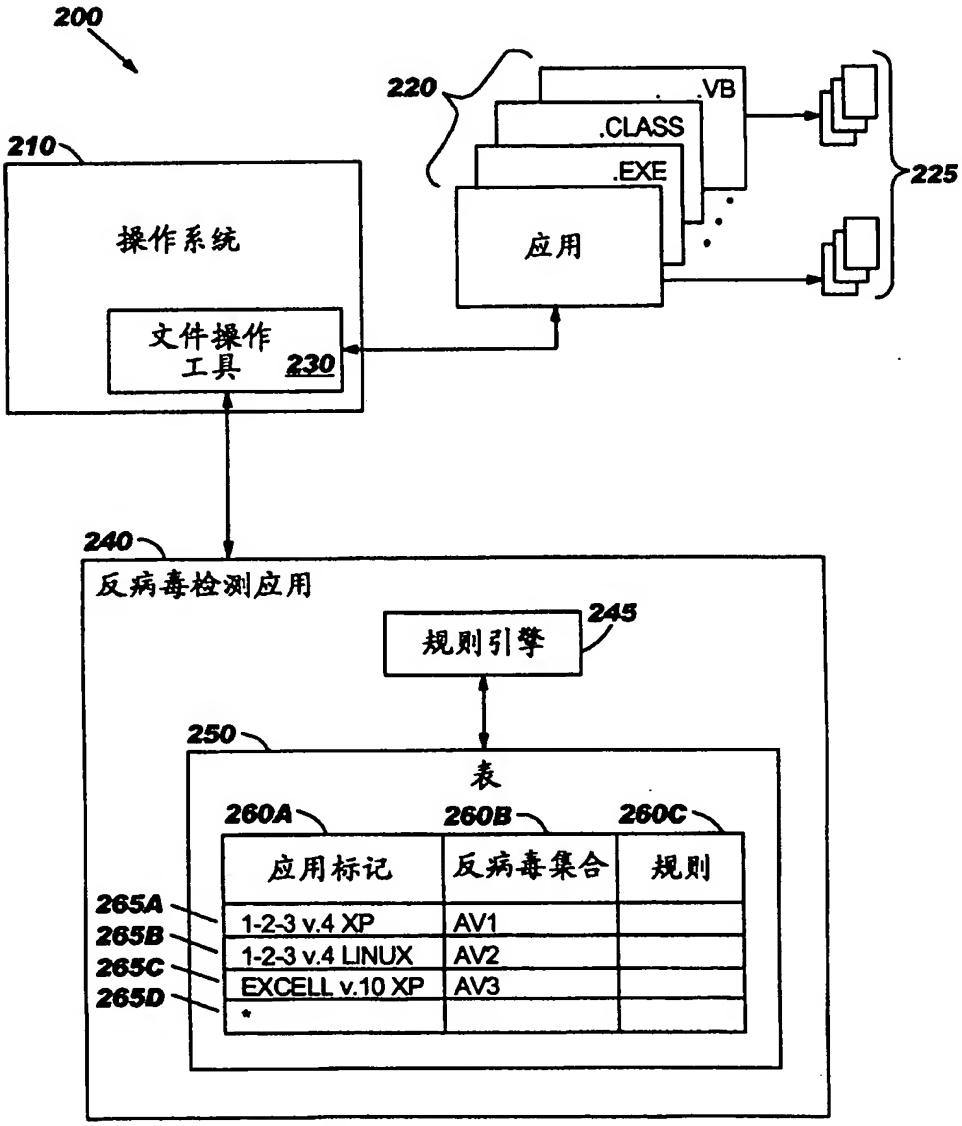

200
220
.VB
.CLASS
.EXE
应用
225
210
操作系统
文件操作
工具 230
240
反病毒检测应用
245
规则引擎
250
表
260A
260B
260C
应用标记
反病毒集合
规则
265A
265B
265C
265D
1-2-3 v.4 XP
AV1
1-2-3 v.4 LINUX
AV2
EXCELL v.10 XP
AV3
*

图3

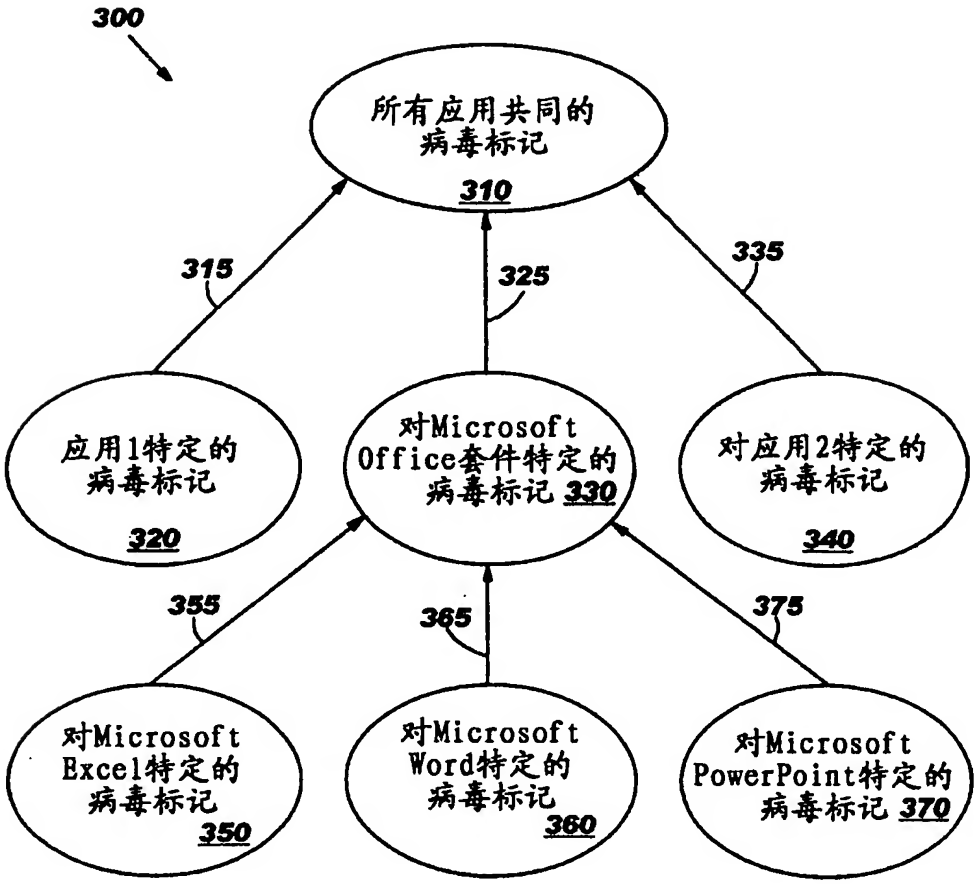
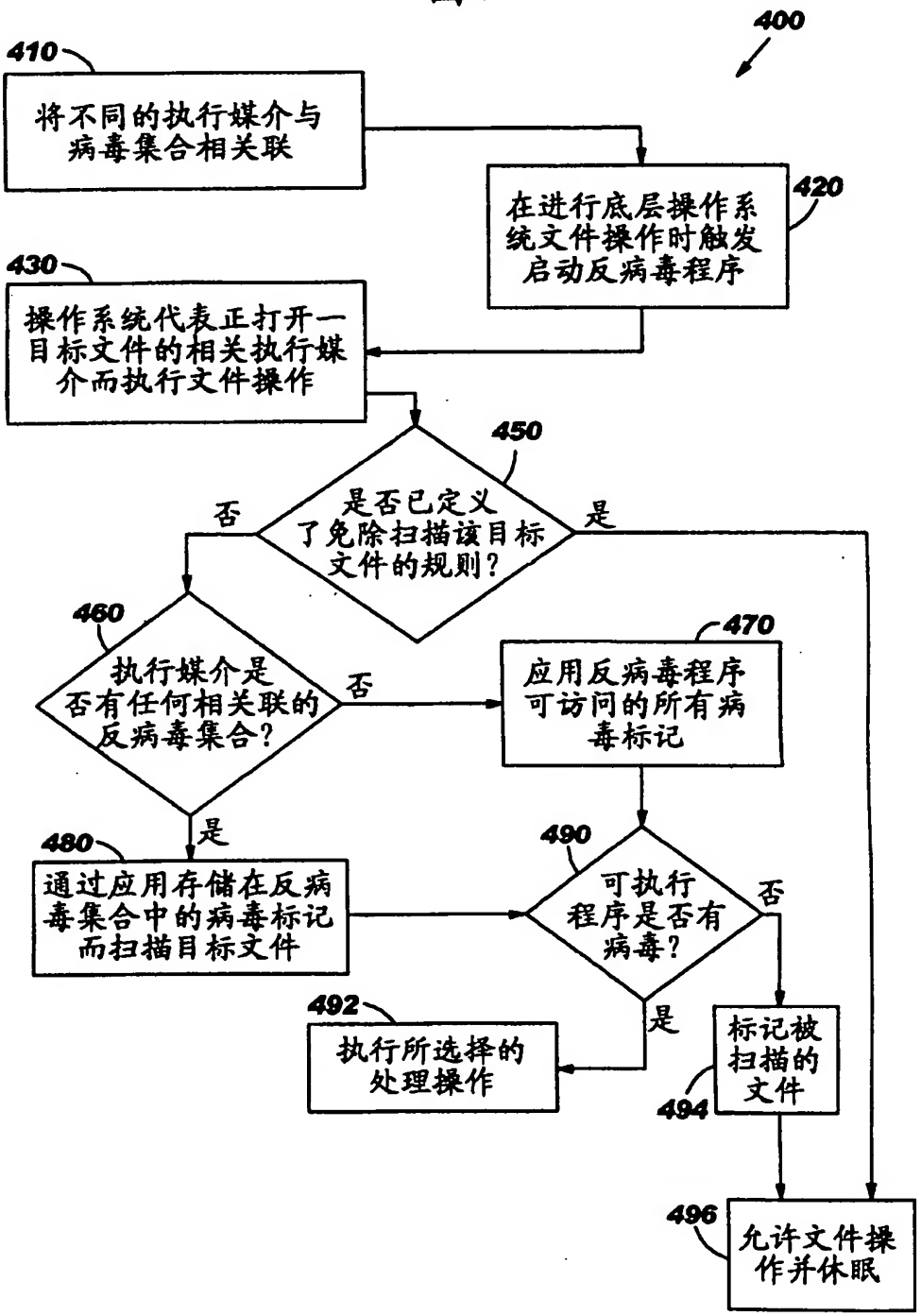

300
所有应用共同的病毒标记 310
315
325
335
应用1特定的病毒标记 320
对Microsoft Office套件特定的病毒标记 330
对应用2特定的病毒标记 340
355
365
375
对Microsoft Excel特定的病毒标记 350
对Microsoft Word特定的病毒标记 360
对Microsoft PowerPoint特定的病毒标记 370

图4


400
410
将不同的执行媒介与病毒集合相关联
420
在进行底层操作系统文件操作时触发启动反病毒程序
430
操作系统代表正打开一目标文件的相关执行媒介而执行文件操作
450
是否已定义了免除扫描该目标文件的规则?
否
是
460
执行媒介是否有任何相关联的反病毒集合?
否
470
应用反病毒程序可访问的所有病毒标记
是
480
通过应用存储在反病毒集合中的病毒标记而扫描目标文件
490
可执行程序是否有病毒?
否
是
492
执行所选择的处理操作
494
标记被扫描的文件
496
允许文件操作并休眠